PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : H04L — A2

(11) International Publication Number: **WO 00/62458**

(43) International Publication Date: 19 October 2000 (19.10.00)

(21) International Application Number: PCT/KR00/00363

(22) International Filing Date: 14 April 2000 (14.04.00)

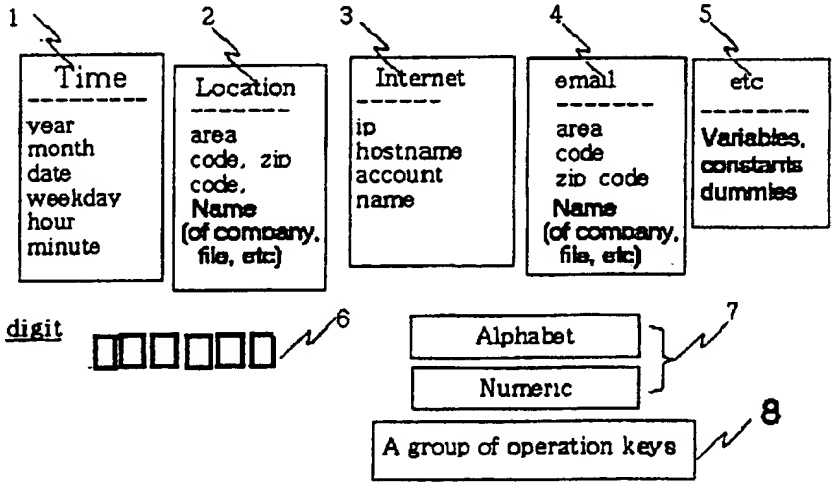
(30) Priority Data:
1999/13182 14 April 1999 (14.04.99) KR

(71)(72) Applicant and Inventor: YU, Choonyeol [KR/KR]; 712-1201 Uruk Apt., Goongrae-dong, Goonpo-si, Gyeonggi-Do 435-047 (KR).

(81) Designated States: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
In English translation (filed in Korean).
Without international search report and to be republished upon receipt of that report.

(54) Title: METHODS AND APPLIANCES FOR ENCRYPTION SYSTEM VARYING DYNAMICALLY DEPENDING UPON VARIABLES AND ITS APPLICATIONS



(57) Abstract

The frequencies of commercial transactions or the kind of activities on a network system have been increased gradually such as transaction with credit cards, connecting onto a banking computer system, usage of vending machines, etc. For this purpose, this invention is a password algorithm system utilizing regularly varying elements such as hour, date, week day, month, etc. that change continuously and other kinds of elements so that the password changes according to the variable elements of time and other elements. In addition, by implementing dynamic variable elements being linked to user's ID, this invention disables the abuse of private information caught by someone on the Internet as ID. Someone who gets the data as ID but not its algorithm couldn't use it as it's not accepted in a server computer system.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

[Description]

Methods and Appliances for Encryption System varying dynamically depending upon variables and its applications.

[Technical Field]

Most of the patents for cryptograph are about ways of encryption/deciphering a specific letter or number so that unrelated persons can not recognize.

A few systems are designed to check the timing element but it's done only on the system and the timing variables are not included within the encryption structure.

There is a ciphering technique called OTP(One Time Password). Once a user connects to a server, the server provides a fixed letter code and the user with the OTP key is to input a password created by the key onto the server. The key generates the password that matches the one the server expects. If the password created by the key is the same with the one on the server, the user is passed on the server successfully. In this case, the will of the user, when creating the password, is not taken into account.

Data is encoded and encrypted to protect it from hacking on the network. Such encryption implies ciphering and deciphering based on a simple algorithm. This invention applies dynamic encryption system to such cryptography.

Most of the existing encryption systems are invariable. That is to say once a password is fixed, the system is designed to keep it. The goal of this invention is to change the password on a regular pattern thereby increasing security enormously.

My dynamic password algorithm, Korean patent application number: 10-1999-0013182 (filed on: '99. 4. 15), utilizes the characteristics of variables and makes the password changed according to the points in time or location so that the secrecy would be maintained, even if the password has been disclosed. The problem with the dynamic password algorithm, however, is that the algorithm set by the user can be ransacked after a user purchases certain products several times at the same on-line shopping mall, leaving considerable amount of data behind on a shopping mall server which is set to log all data the user puts in. But, in this invention, the means for user identification such as id uses this dynamically varying system and thereby it makes harder or impossible to grasp how the algorithm is structured at the shopping mall.

None of the existing calculators have such function as inputting dynamic variables.

Furthermore, while the data are saved alphanumerically on credit cards, this invention stores data in the form of arithmetic functions reads in these data and calculates the arithmetic functions utilizing the dynamic variables and eventually have the calculation results displayed or put in automatically on the networks.

[Background Art]

Eliminates dangers following password disclosure by changing it regularly.

Especially in the situation when paying for buy on the internet, removes the dangers following revelation of information and also decreases feelings of uneasiness.

Enables the user to apply the same password with a plurality of credit cards.

Makes the password hard to be broken by linking the dynamic variables with alphanumeric strings, numeric constants, etc utilizing arithmetic operators, linking operators, etc.

Despite the usage of dynamical password, one can acquire the formation of the password by comparing/analyzing 2 or more passwords. This invention solves and improves this problem to great extents.

Apart from the natural elements like time and location that vary naturally, there could be artificial elements created by the user using computer functions. In other words, in accordance with a message issued for a basis, encryption is formed and accordingly the password is to be entered. This invention is designed to include the various kinds of variable elements.

This invention is to have users set the password according to the algorithm of this invention, then encrypting the data entered as a password with the existing cryptographic encryption algorithm and finally reversely decrypting it.

Processing data through dynamic password system, the data is ciphered.

Some troubles can arise, as it is required to calculate the password data to be entered based on the password algorithm even though the dynamic password is set complicatedly. This is to be solved by arranging hardware calculator system.

This invention is to make a hardware lock systems such as a door

lock utilizing the basis of this dynamic password algorithm.

Adapting the dynamic password onto the network can help in improving the demerits of public protocol. In spite of data hacking, if the data were not received through the dynamic password algorithm agreed between hosts and were not decoded through NIC(Network Interface Card), the data would be closed up eternally. Such system should be adopted onto NIC.

Forming the dynamic password system diversely, the problems within the existing password system can be solved.

Apply this password system in various practical fields and to existing password/encryption/decoding systems.

Draw up a device that makes it impossible to confirm the user even if the data he/she entered using dynamic password system and it is logged by a computer system.

Derive a scheme to avoid ID overlapping.

Develop a device that can calculate arithmetic equations easily of the dynamic password system. Such device would either consist of both input and output functions or forms in the kinds of systems consisting of one or all of functions of input, calculation or output. The latter would be lighter and easy to carry.

[Disclosure of Invention]

This invention utilizes and selects the elements that vary according to the point in time. Needless to say, the elements would be all variable elements including the point in time, the point in location of payment/transaction being made, etc. The time elements include year, month, day, the day of the week, hour, etc. Location elements are distinguished by the nation, state, city, district, etc that are the basis of exact location of the payment/transaction (called 'variable elements' hereinafter). Usage of these elements enumerated above that continuously change, has great effect as it can prevent crimes.

As the elements to use are selected, in supplementing constant password or static password(hereinafter called 'constant elements') this invention uses arithmetic operation with addition, subtraction, and other variable computation elements' (hereinafter 'computation elements').

Variable elements are as follows.

- Year: y1y2y3y4 (y for the number of the year. The number means digits. Example: 1999)

- Month: m1m2 (m for the number of the month. The number means digits. Example: 04)

- Day: d1d2 (d for the number of the date. The number means digits. Example: 27)

- Hour: h1h2h3h4 (h for the number of the hour. The number means digits. Example: am07, pm04, 07am, 04pm, 13, 23)

- The day of the week: sun....sat or 0....6 ('sun'....'sat' or '0'....'6' are the abbreviation of the weekday or are the number codes representing the day of the week)

Codes for Locations: National codes, states, city, county, and district codes. Telephone code, zip code, file number of a computer, etc. (Examples: Korea, USA, Australia, of49, 012, 02, 0343)

Codes of/for Firm names, Internet addresses, etc: 2haho, mygem, pascal, www.molab.co.kr

The following is an example of passwords of this invention using variable elements, constant elements and operators.

[Table 1]

Example of dynamic passwords

Example		1	2	3	4
Variable element		y1y4	y4m2	weekday	y3
Computation elements		* 3	+ 25	+ 11	+ 34
Method of adding constant elements		.	+	.	.
Variable element		The first 2 letters of the firm name on the web	The last 2 digits of the zip code		h1h2m1m2
Method of adding constant elements		.	.		.
Constant elements			cat12	123	Not
Inputted password	(1)	572h	166cat12	Svo123	430930not
	(2)	60mo	128cat12	tvf123	342325not

Calculations for the inputted password	(1)	Ycar 1999 = 19 * 3 =57 firm name on the web = '2haho'	Ycar 1999 April(04) = 09 + 04 = 94 + 25 = 119 zip code: 435-047 119 + 17 = 166	sun + 011 = svo(adds ascii code 1 to 'u' and 'n')	Ycar 1999 0930 = 9+ 34 = 43 h1h2 = 0930
	(2)	Year 2000 = 20 * 3 = 60 Firm name on the web = 'molab'	Year 2000 June(06) = 06 + 25 =31 Zip code: 023-497 31 + 97 = 128	tue + 011 = tvf	Year 2000 2325 = 0 + 34 = 34 h1h2m1m2 = 2325

In the example above, the positions of the variable element and constant elements can be changed and the elements may be used more than once. Example: weekday. (3h4 x 2). m2

If the keyboard does not allow input of English alphabets, the constant password can be formed of numbers only.

The method of adding constant elements is by using operators of a computer language. In the example above, '.' is the string operator for interconnection between letters, words.

The inputted password means the actual password to be inputted.

As one can observe in the example above, the password changes according to time and utilizes the arithmetic operations and others and it makes it impossible to connect to the system using the same password again. It is safe even if the password has been disclosed on-line temporarily and the users are relieved of worries about password disclosure at shopping malls as the password changes at next time.

The weak point of this invention is that one can notice the formation of the password structure if 2 or more passwords were to be compared and analyzed. Therefore, a dummy digit is implemented in addition to complement such demerits. Namely, if the whole password consists of 8 digits, 4 digits would be of variable password, 2 digits of the constant password and the rest 2 digits of the dummy. The dummy password has no

meaning what so ever and only acts to prevent the algorithm from being analyzed. That is to say, 23 inputted today, ac tomorrow, 7b the day after tomorrow and so on. The computer ignores these dummy digits no matter what they are.

To set a password using this invention, it requires separate processes of or structures for setting each of variables, constant elements and operations. In addition, there arises the problem of calculating the password one by one if the password was set extremely complexly. For such usages, the hardware system of the password generator is devised so that it would be easy to set, select, calculate and input passwords. As shown, 1, 2, 3 and 4 in Fig. 1 are the keys for selecting the variable password element, 5 is for selecting the constant element and the dummy digit. 6 is the key that determines the number of digits of the password, key 7 is a key that changes variable elements into alphabets or Arabic numbers. Key 8 is a group of keys required to link the dynamic variable elements and constant elements through arithmetic operators (+, -, *, /, etc), logic operators, string operators, etc. It includes numeric input keys of 0 ~ 9 and alphabet input keys if/when required. It consists of the numeric number keys of 0 to 9 and if required the alphabet keys are to be included as well. This password generator includes keys of operator for arithmetic operations, logic operations and other operations as used in a computer language. To form such automatic password calculator/generator, the capability of the CPU has to be implemented.

Fig. 2 is a a flow chart depicting how the password is set.

Variable elements can be artificial elements let alone natural elements like time and location.

When connecting to a server, the server can provide the user with a certain type of message or combination of letters on a display monitor or transmit to a user, then the user thereby accordingly does performing some operations linking certain letters and/or inputting the result directly.

With this invention, it is possible to break down the timing variables into minutes, seconds, or even nanoseconds, etc.

It is possible not only to utilize varying 'the time' as is as a password or further but also to make a various encryption system to the extent of whatever wanted with high security system by utilizing timing factors sub-divided into further detail to nanosecond or further as variable elements based upon the time when connecting to a server. The user, of course, can use the already existing static password instead of the dynamic one. It's impossible to calculate or input manually the password generated

adopting the expanded password into nanosecond. In this case, the server would provide or convey the dynamic variable elements to a password generator, so that the generator receives the data and generate a password according to the password generation algorithm pre-set on a password generator. The password generator displays the calculation result or input it to a server remotely.

Arithmetic equation for dynamic password ranges from elementary calculations to various arithmetic theories such as differential calculus, integral calculus, etc. It can even be arranged so that the x-axis on the coordinates represents the time variable of the password, while the y-axis represents the real password resulted in calculation to be inputted.

This dynamic password system can be implemented on a network. The hosts would set a password in advance using dynamic password system, and by reusing the dynamic password system, one of the hosts codifies and transmits data to the other host. Then, the host with the received data would decode and/or decrypt utilizing the dynamic password system according to the algorithm and/or decoding/decryption algorithm pre-defined and pre-set. For example, two hosts would set a specific password beforehand. The flowing data on the network, if not received by the host's NIC and acknowledged by it, would vanish normally. If it has been hacked, on the other hand, the data would remain constantly on a hacker's computer system and the hacker using this information would keep try hacking. In a computer systems equipped with the dynamic password system of this invention, however, encrypt and/or encode data with encryption algorithm implementing elements of time and location factors such as ip address. Thus, unless the data is decrypted in a limited set time by NIC, it becomes impossible forever to decrypt it caught by a hacker. The data that is encrypted or ciphered in a new data format according to timing elements and transmitted next time cannot be compared either as it is codified with new timing variables. Adding such functions to a NIC hardware would result in forming an improved security network adaptor card.

Forming hardware systems applying the dynamic password algorithm is essential. A hardware security device like door lock can be made consisting of CPU, screen display device, input unit, and data storing unit. The Screen displaying device can be omitted and the input unit can be designed to input data remotely.

There could be many different ways, using dynamic methods, in making passwords so that it would be hard to decrypt data encrypted or a

password. This enhances the security to great extent.

- Forming passwords by changing the places of digits of fixed and variable passwords regularly, and setting the pattern of the change methodically. In other words, the fixed password, for example, 1234 can be changed according to day of the week, date, hour to 1324, 1432, 3214.

- Alternating fingers to be used on a fingerprint recognition system on a daily basis. That is to say, the print of the thumb used on Mondays, the print of the second pointing finger on Tuesdays and the third middle finger for Wednesdays and so on.

- Alternating the encryption and decryption algorithm for a voice recognition system so the password is changed periodically and regularly.

This Invention applies to all kinds methods that are used in ciphering data, whether it is based on naturally changing elements or artificially changing elements of the variable.

This Invention uses the dynamic password algorithm in the same way onto IDs that are used in confirming the user. Namely, it uses the dynamic password algorithm in the means for identifying the user (hereinafter called 'id'), this invention uses a dynamically varying variables as an id. Such variables include the naturally changing elements and the artificially changing elements that I have mentioned so far. If the IDs were to be set with this algorithm, there is a possibility of having identical IDs coming out made up of same numbers or alphabets. This problem, however, complicates nothing if identical numbers are not generated in simulation that at the same point in time the timing variables are applied to many password algorithms. Assuming that "A" uses the hour" and "second" timing variables in his/her dynamic ID algorithm and "B" does "day" and "hour" variables. We can identify individuals without any problems if the resulting ids coming out in calculation are not the same at the given point in time. As A's password is based upon 'second', the number of password in a given period of time is more than ones generated using B's algorithm which used 'hour' element. Thus, during the given period of time, not at a given point in time, the same result ids may be generated of A's and B's.

The ways to prevent such ID collisions (hereinafter called 'id collision) are :

1) Set regulations of making " 10 minutes" as the minimum timing variable.

2) It's mandatory for all users to use the "second" variable.

3) Applying an static constants to particular digit(s) can evade such problems. If identical IDs are created, looking at this static constant can

identify each user.

As passwords are set distinctly together with an id ultimately, the possibilities of having identical ID and password at the same time are enormously rare. When determining the ID, the computer systems have to check by calculating and generating his/her ID and password with the algorithm and check if identical ones exist. Such calculation and checking doesn't have to be done as of present but can be performed in past point in time, for example, "1945 November 23 12:36:38". The calculation records are kept in a computer system and compare a new one with it to for check purpose.

This dynamic id, as in the same as a dynamic password system, consists of a basic ID, dynamic variables and static constants and calculates the data of the real id to enter using arithmetical equations.

Furthermore, the user can carry a magnetic card in which the basic ID, the variables and the arithmetical equations are stored so that the result password or id can be automatically calculated and inputted.

[Brief Description of Drawings]

Fig.1 shows the basic block structure of this invention.

Fig.2 shows the flow chart illustration the process of dynamic password algorithm setting and calculations.

[Best Mode for Carrying Out the Invention]

Described in the above 'Disclosure of Invention.

[Industrial Applicability]

Even if the user ID and password are recorded/logged on a computer system, ID itself constantly changes thereby making it impossible to figure out the structure of a password and id algorithm.

It is possible to produce the actual value to enter in a computer system for user identification by using variables and the arithmetic operation. The input, output and calculating functions can be either all formed into a system or can be implemented into each of separate systems respectively so that it would be easier to use it carrying.

Making purchases on the Internet is now the general tendency and it is estimated that such on line transactions in this tendency will be expanded further on the grounds that distribution cost decreases resulting in cheap buying costs. Although many Internet users acknowledge such merits and want on-line transaction, they hesitate because of the possibilities of subsequent disclosure of private info. Such as credit card number and the password on a shopping mall, stealth and illegal abuse of those info, etc.

Today, there are many statistics showing worries over password

exposure that is the main reason for avoiding on-line purchases.

Besides, the existing password system has fixed static passwords so that once the password is disclosed, it requires changing. It is inconvenient that the staffs at banks and shops ask the clients about the credit card's passwords and sometimes have to cover up so that no one would see worrying exposures.

As this invention utilizes an algorithm having data to enter such as a password, etc changed being varied, even though such a password is disclosed, if others, who caught the password number, not knowing the structure of the algorithm of a password, couldn't get passed in a banking server in different time and in different location. Accordingly, no need to worry about password disclosure.

Many online transaction solution providers suggest hardware solutions such as a smart card, etc to troubleshoot this problem. It costs a lot such card makers and users in buying hardware systems. It causes the wastes of resources. This invention can be adopted very easily and simply by changing/modifying login password programs in a computer systems. The hardware solution contains the possible risks of stealth, copy or theft. This invention has no such risks. If incorporated into a hardware system such as a smart card, it intensifies the security to a great extent.

If a password is set complicated, the data value to enter can be generated easily using a password generator. Also, the password generator may be designed to get a transmission of resource data such as variable elements, etc remotely and automatically and generates a password to enter and finally transmits it to a server for entry.

This invention provides various password algorithm such in the form of existing fixed static password, of simple dynamic password algorithm set like 'month x hour' or of a dynamic password algorithm set precisely to the extent to nanosecond or further meeting users' various requirements. This expands the user coverage greatly and diversely.

This invention eliminates the dangers of password disclosure. It will help on-line purchases with credit cards.

If the dynamic password system were to be adapted to the network, it will improve the existing problems of hacking of open protocols such as TCP/IP, etc. This is the way to remove the defects of TCP/IP. Adopting such functions to network cards would result in a intensified network device. And the variable network elements would be not only natural elements such as time and location but also artificial elements. Namely, when connecting to a server, the server can provide the user with a certain

type of message or combination of letters on a display monitor or transmit to a user, and then the user thereby accordingly does performing some operations linking certain letters and/or inputting the result directly.

Adopting this dynamic password algorithm to the existing password system additionally intensifies security to great extents.

[Claims]

[Clause 1]

It is made up of password unit and variable elements that are artificially created or that change according to a regular pattern set by the user. It is a coding/decoding system that uses such variable elements in connection to the password unit.

[Clause 2]

As for clause 1, the natural variable elements include the passing of the time, the change in location, the account of the user, while the artificial elements are produced and displayed by the computer for the user to make reference to. This variable coding/decoding system has such features.

[Clause 3]

As for clause 1, the variable elements can be combined using arithmetical logic units. This variable coding/decoding system has such features.

[Clause 4]

As for clause 1, the password unit is formed of letters and is to be compared with other password systems that are stored using letters. This variable coding/decoding system has such features.

[Clause 5]

As for clause 1, the password unit is a fingerprint recognition system designed to recognize the fingerprints and compare it to the fingerprint data that is saved. This variable coding/decoding system has such features.

[Clause 6]

As for clause 1, password-complicating unit is included additionally with the other password elements mentioned to intensify security. This variable coding/decoding system has such features.

[Clause 7]

As for clause 6, the password-complicating unit includes a dummy digit that is not used by the computer when decoding. This variable coding/decoding system has such features.

[Clause 8]

It is made up of an input unit, CPU and data storage unit and the input unit is enabled to enter variable elements, whether created naturally or artificially. It is a variable password generator as it creates a value by conversing the inputted data.

[Clause 9]

As for clause 8, a remote input unit inputs the data. It's a variable password generator with such features.

[Clause 10]

As for clause 8, input keys exist for the user to enter variable elements mentioned above manually by using the input unit. It's a variable password generator with such features.

[Clause 11]

As for clause 8, the natural variable elements include the passing of the time, the change in location, the account of the user, while the artificial elements are produced and displayed by the computer for the user to make reference to. It's a variable password generator with such features.

[Clause 12]

As to coding/decoding of data, the system is designed to cipher data in accordance with variable elements, whether created naturally or artificially.

[Clause 13]

As for clause 12, the natural variable elements include the passing of the time, the change in location, the account of the user, while the artificial elements are produced and displayed by the computer for the user to make reference to. This is the characteristic of the system for coding/decoding of the data.

[Clause 14]

As for clause 12, the variable elements can be combined using arithmetical logic units. This is the characteristic of the system for coding/decoding of the data.

[Clause 15]

As for clause 12, password-complicating unit is included additionally with the other password elements mentioned to intensify security. This is the characteristic of the system for coding/decoding of the data.

[Clause 16]

As for clause 15, the password-complicating unit includes a dummy digit that is not used by the computer when decoding. This is the characteristic of the system for coding/decoding of the data.

[Clause 17]

A variable password lock device constituted of CPU, data storage unit and input unit, the data entered through the input unit and saved at the data storage unit so that it is possible to create passwords according to the variable elements, whether created naturally or artificially. Such data would be checked to see if it's formed fairly by the data-storing unit.

[Clause 18]

As for clause 17, the variable password lock device would include a display unit additionally in order to show the user the data put in.

[Clause 19]

As for clause 17, the input unit can be either a remote one or a one with keys to be entered manually.

[Clause 20]

As for clause 17, the natural variable elements include the passing of the time, the change in location, the account of the user, while the artificial elements are produced and displayed by the computer for the user to make reference to.

[Clause 21]

As for clause 17, the variable elements can be combined using arithmetical logic units.

[Clause 22]

As for clause 17, password-complicating unit is included additionally with the other password elements mentioned to intensify security.

[Clause 23]

As for clause 22, the password-complicating unit includes a dummy digit that is not used by the computer when decoding.

[Clause 24]

A data coding/decoding device that is made up of CPU and a data coding/decoding unit, codes/decodes data based upon variable elements that are created naturally or artificially.

[Clause 25]

As for clause 24, the data coding/decoding unit is saved in a data-storing device and is included additionally in the data coding/decoding device.

[Clause 26]

As for clause 24, the natural variable elements include the passing of the time, the change in location, the account of the user, while the artificial elements are produced and displayed by the computer for the user to make reference to.

[Clause 27]

As for clause 24, password-complicating unit is included additionally with the other password elements mentioned to intensify security.

[Clause 28]

As for clause 27, the password-complicating unit includes a dummy digit that is not used by the computer when decoding.

[Clause 29]

A fingerprint recognizing system designed to compare fingerprint with the already-set fingerprints for security reasons, is formed of many fingerprints stored in its storing unit and the variable elements that are both natural and artificial. By relating the variable elements and the stored

fingerprints, the system is designed to accept different prints for each variable.

[Clause 30]

1. A variable ID system where the continuously changing variable is applied to methods of confirming the user so that the IDs also change.

2. As for the clause 1, the variables change according to time and

3. As for the clause 1, according to shift in locations.

4. As for the clause 1, the variables mentioned include the artificially set ones.

[Clause 32]

1. A variable ID system where the continuously changing variable is applied to methods of confirming the user so that the IDs also change.

2. As for the clause 1, the variables change according to time.

[Clause 33]

1. A variable ID system where the continuously changing variable is applied to methods of confirming the user so that the IDs also change.

2. As for the clause 1, the variables change according to shift in locations.

[Clause 34]

1. A variable ID system where the continuously changing variable is applied to methods of confirming the user so that the IDs also change.

2. As for the clause 1, the variables mentioned include the artificially set ones.

[Clause 35]

1. A variable calculating device where the constantly changing element is set as the variable clause, and this variable clause includes numbers, numbers that possess alphabets as numeric digits. Made up of units that make it possible to input general arithmetical function symbols, it allows the calculation functions.

[Clause 36]

1. A variable data saving device where the constantly changing element is set as the variable clause, and this variable clause includes numbers, numbers that possess alphabets as numeric digits. It stores data of the arithmetic equation using general arithmetical function symbols.

2. As for the clause 1, the data is saved in a magnetic mode.

[Clause 37]

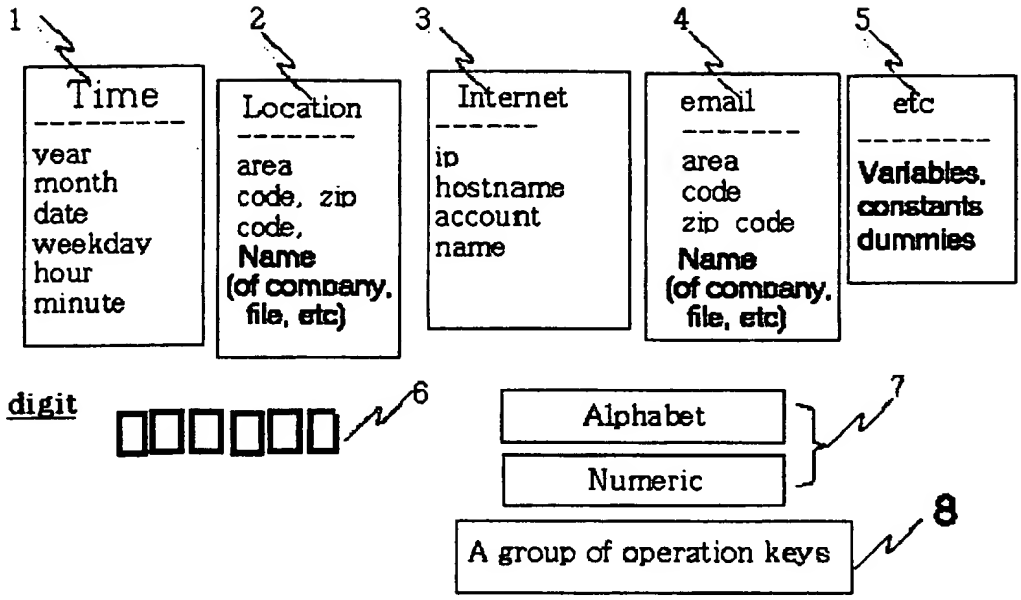
1. A variable data calculating/deciphering device where the constantly changing element is set as the variable clause, and this variable clause includes numbers, numbers that possess alphabets as numeric digits.

It stores and deciphers data of the arithmetic equation using general arithmetical function symbols and can acknowledge such variable clause.

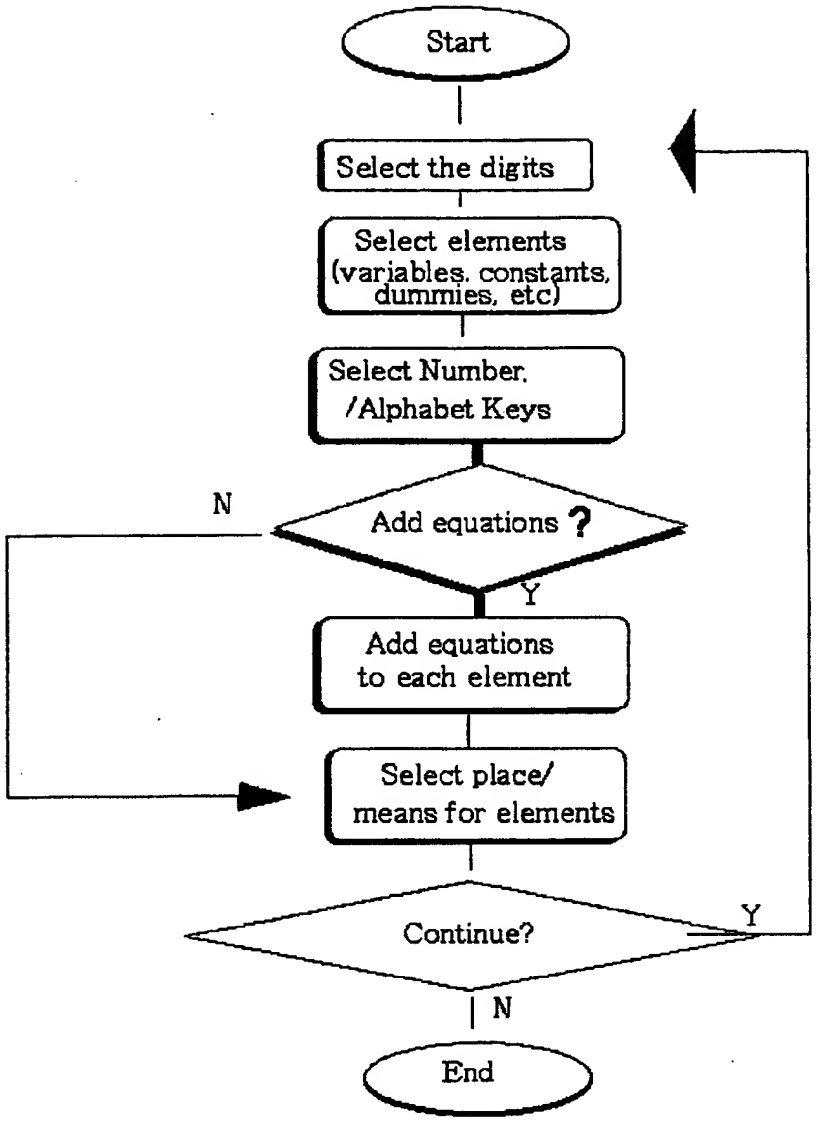
2. As for the clause 1, a variable data calculating/deciphering device can read magnetic data, as the data mentioned is formed in magnetic mode.

[Drawings]

[Fig. 1]



[Fig. 2]


Start
Select the digits
Select elements (variables, constants, dummies, etc)
Select Number, /Alphabet Keys
Add equations ?
N
Y
Add equations to each element
Select place/ means for elements
Continue?
Y
N
End

5